
Setup guide for DeepL Single Sign-On (SSO)

SAML: Microsoft Entra ID (formerly Azure AD)

Table of contents

[Requirements](#)

- [1\) Open Azure AD management](#)
- [2\) Register enterprise app](#)
- [3\) Configure assignment](#)
- [4\) Configure initial settings](#)
- [5\) Claims and Attributes](#)
- [6\) Download the Metadata XML](#)
- [7\) Provide data](#)

Requirements

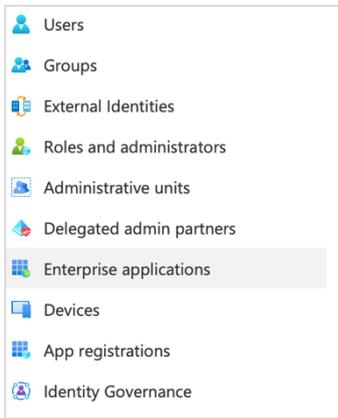
- You have an Azure AD set up
- You have administrative permissions to create an app within the Azure AD tenant
- A company domain has been defined for the DeepL environment. For further information please check our [Help Center article](#).

1) Open Azure AD management

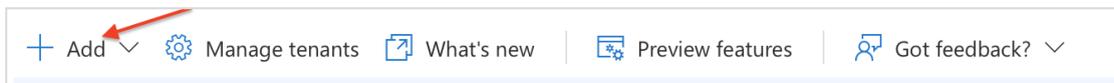
- Open <https://portal.azure.com> and select *Azure AD*. The direct link is https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview

2) Register enterprise app

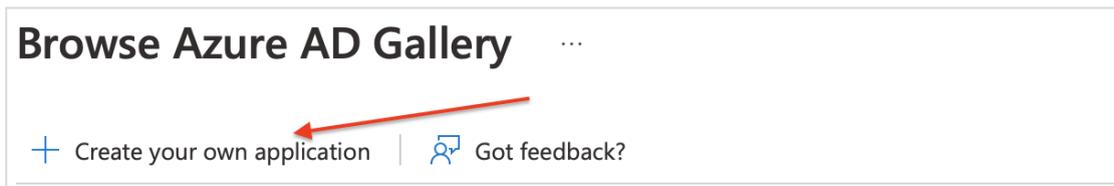
1. Select *App registrations* in the left-hand menu



2. Click *Add* on the top panel



3. Click *Create your own application*

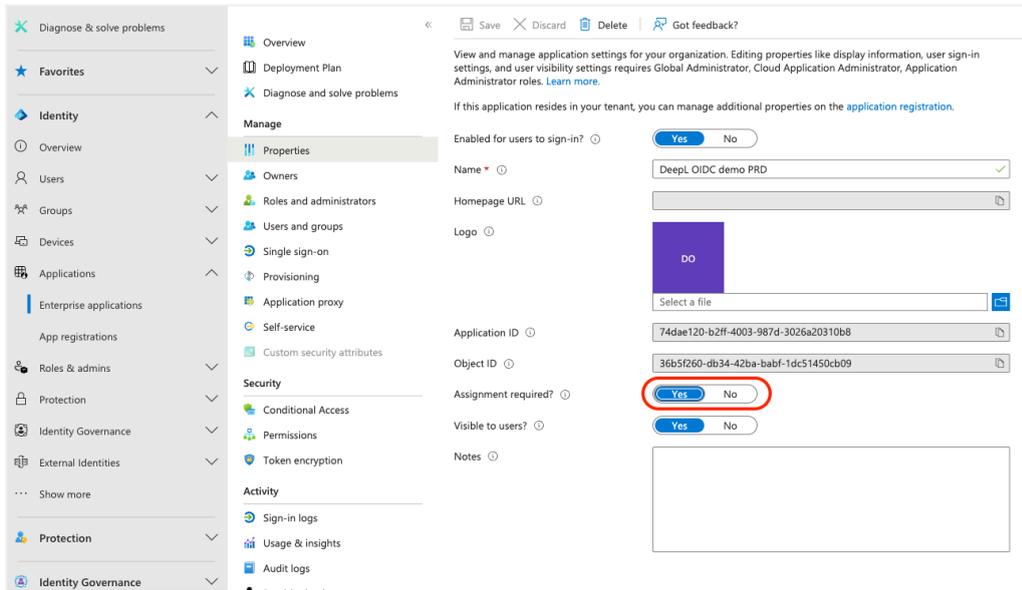


4. Create a Non-gallery app

A dialog box titled 'Create your own application'. It includes a 'Got feedback?' link, a descriptive paragraph, a text input field for the app name (containing 'DeepL Pro'), and three radio button options for the app's purpose. The 'Integrate any other application you don't find in the gallery (Non-gallery)' option is selected. A 'Create' button is at the bottom.

3) Configure assignment

1. Select *Enterprise applications* in the left-hand menu
2. Choose the application that has been created automatically
3. Select *Properties* in the left-hand panel
4. Set *Assignment required* to *Yes*



4) Configure initial settings

1. Click on *Set up Single Sign On*

Getting Started

 **1. Assign users and groups**
Provide specific users and groups access to the applications
[Assign users and groups](#)

 **2. Set up single sign on**
Enable users to sign into their application using their Azure AD credentials
[Get started](#)

 **3. Provision User Accounts**
Automatically create and delete user accounts in the application
[Get started](#)

 **4. Conditional Access**
Secure access to this application with a customizable access policy.
[Create a policy](#)

2. Edit basic SAML configuration

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating DeepL Pro .

- 1 Basic SAML Configuration**

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional
- 2 Attributes & Claims**

⚠ Fill out required fields in Step 1

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

- Set the Entity ID to `https://w.deepl.com/auth/realms/prod`
- Set the Reply URL to `https://w.deepl.com/auth/realms/prod/broker/ALIAS/endpoint`

Replace ALIAS* with your chosen Company SSO domain and save the set values.

Basic SAML Configuration

Save | Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

ⓘ

[Add identifier](#)

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index Default

ⓘ

[Add reply URL](#)

* ALIAS value can be found under Company SSO domain in SSO configuration area

5) Claims and Attributes

- Set the claims and attributes:
 - email address
 - givenname
 - surname

Please use following Microsoft default claim for each attribute for the set up in the DeepL interface.

2 Attributes & Claims Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

6) Download the Metadata XML

- Click on *Download* for Federation Metadata XML

3 SAML Certificates Edit

Token signing certificate

Status	Active
Thumbprint	26312E3715BBCD3CB3003E194EFC38196B6A98A3
Expiration	2/6/2026, 9:25:03 PM
Notification Email	marquistore@googlemail.com
App Federation Metadata Url	https://login.microsoftonline.com/c4831599-357f-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

[Download](#)

Verification certificates (optional) (Preview) Edit

Required	No
Active	0
Expired	0

7) Provide data

Provide the following data in your DeepL Account settings:

- Federation Metadata XML:
 - By uploading the XML file
 - By entering the location (URL) of the XML files URL in your identity provider
- NameID policy format: Email

- Set the attributes:
 - First name: <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname>
 - Last name: <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname>
 - Email address: <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress>

Authentication type

SAML ▼

Configure SAML

You can import external IDP metadata from a config file or from a URL. The administrator of your identity provider is the best contact person for the required information.

Import from URL ?

Import from file ?

*.xml format

NameID policy format

Email ▼

Assertion attribute: First name ?

Assertion attribute: Last name ?

Assertion attribute: Email address ?